

AGENDA

General Security Issues

1. Welcome / Introduction (Cindy)
2. Updates on the security website (Cindy)
 - a. Updated the MAIN FACS Security Administration Monitoring Checklist (*see handout*)
 - b. Updated B.O. Corporate Document Listing
 - c. Add information for DSA
 - d. Other – Intranet
3. MIDB Statewide User Annual Certification – Completed (Cindy)
4. Updates on Business Objects (Cindy/Art)
 - a. Security Request Forms Drafts (*see handout*)
 - b. Access to Security Universe
 - c. BO Password Reset Training
 - d. BO Password Reset Only Access
 - e. BO Password 30 Day Expiration Issues (Art)
 - f. Other
5. MAIN FACS security framework
 - a. Due March 1, 2009
 - b. Update as needed for changes
 - c. Incompatible memos
6. Other comments

Business Objects Reports (*see handout*)

1. MAIN FACS: SEC 24 – (RACF) User IDs and Job Changes/Process Level Changes
2. RSTARS: SEC 30 – (RStars) Security User Class Conflicts
3. ADPICS: SEC 04 – (AP) Summary of ADPICS Sec by User ID
4. MIDB: SEC 17 – (MIDB) Roles by User
5. Other Reports: SEC 42 – (MASTER) User ID's by Employee
6. Other Comments

BUSINESS OBJECTS WORKGROUP &
AGENCY SECURITY ADMINISTRATORS MEETING
SEPTEMBER 18, 2008

SESSION NOTES

The following is a summary of the materials covered in the meeting:

Updates on the Security Website

We have updated the MAIN FACS Security Administration Monitoring Checklist on the security website (http://www.michigan.gov/documents/checklist_6_15_04_97402_7.doc) and a hardcopy of the list was distributed during the meeting. All the reports listed in the checklist are now available. ASAs should refer to this checklist to ensure proper monitoring of their users' security. ASAs can also use the list for preparing the 2009 framework. We have also updated the BO Corporate Document Listing on the security website (http://www.michigan.gov/documents/budget/Business_Objects_201466_7.doc). Some new reports have been added to the list since the last ASA meeting in July. We will add more information for DSAs on our website in the near future.

MIDB Statewide User Annual Certification

The MIDB Statewide User Annual Certification review is completed. We made some changes to the certification form, per request from some ASAs, so next year the form will be more user friendly.

Updates on Business Objects

We distributed the draft of the updated B.O. Security Forms during the meeting and ASAs agreed with the changes with some minor modifications.

DSAs will need to be granted access to the BO Security Universe to utilize the DCDS monitoring reports. ASAs should be receiving the requests in the near future.

Art taught 2 sessions of the BO Password Reset class on 9/8/08 and 18 ASAs and backups attended the classes. The final session will be held on 9/22/08 and Jim Edwards will teach it. All the ASAs and backups have already been granted the rights to reset passwords. There is a self-study available on resetting BO passwords. If you would like the information, email Art.

Upon request from ASAs, we can also grant BO Password Reset Only Access.

In the current BO version, the password expires after 30 days without warning the users. This issue will NOT be changed until at least the next version upgrade. Users have to remind themselves to change the password within 30 days. Otherwise, they will need to have their passwords reset.

BUSINESS OBJECTS WORKGROUP &
AGENCY SECURITY ADMINISTRATORS MEETING
SEPTEMBER 18, 2008

MAIN FACS security framework

Cindy reminded the ASAs that the MAIN FACS security framework for 2009 is due March 1, 2009. ASAs can also update the 2008 framework anytime, as needed. Cindy re-emphasized that the incompatible memo should be submitted for every user with incompatible UCs.

Business Objects Reports (see handout)

- **MAIN FACS: SEC 24 – (RACF) User IDs and Job Changes/Process Level Changes.** This new report identifies User ID's that belong to employees who have had a job change (within the agency or moved into the agency). ASAs should review and determine if access is still appropriate for their new job function. ASAs may need to contact the ASA from the former agency of the transferred employee to identify the need for access change. We recommend that ASAs run this report bi-weekly.
- **RSTARS: SEC 30 – (RStars) Security User Class Conflicts.** This new report has 3 tabs and it identifies the users with conflicting RSTARS UC combinations. The first tab identifies the users with incompatible user class assignments in RSTARS. ASAs should review the report, verify that access is still needed, and ensure all the users on the list are covered by the incompatible memos. The second tab identifies the users with undesirable UC assignments and the third tab identifies the users with illogical UC assignments. ASAs should review the 2 reports and verify that access is still needed and appropriate. ASAs should obtain assurance that compensating controls are in place to address risks associated with the conflicting UC assignments. The report is also very helpful for updating agency security frameworks. We recommend ASAs run this report quarterly.
- **ADPICS: SEC 04 – (AP) Summary of ADPICS Sec by User ID.** This report provides the ADPICS users' security profile (e.g., user classes, document/document types, user departments, mailbox departments, department authorizations). ASAs should coordinate a review of all users' security privileges in ADPICS to determine if access is still appropriate for users' job functions. We recommend ASAs run this report quarterly.
- **MIDB: SEC 17 – (MIDB) Roles by User.** This new report provides all the BO users with statewide access. We are working on expanding this report to also provide lists for users with Most Agencies and/or Agency Only access. ASAs should review users' security privileges in BO to determine if access is still appropriate for the users' job functions.
- **SEC 42 – (MASTER) User ID's by Employee.** This new report provides a list of users with IDs in ADPICS, RSTARS, DCDS, MIDB, MAP, and HRMN. ASAs should review the users' security privileges in BO to determine if access is still appropriate for users' job functions.